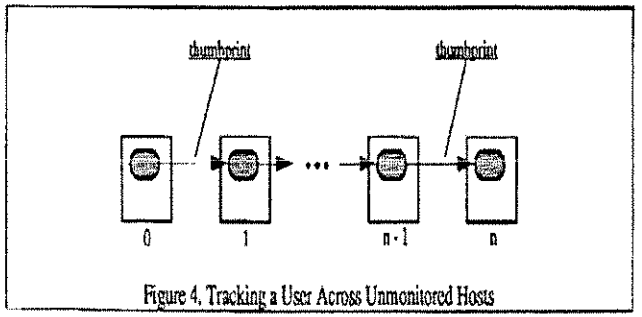
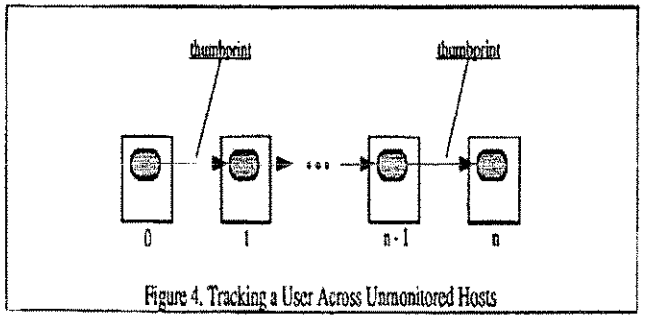
Internetwork Security Monitor
"ISM"

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
		[SYM_P_0069250-SYM_P_0069251] "4.2.2 THUMBPRINTS The NSM maps host-to-host connections to an extended connection by assigning to each host-to-host connection a thumbprint representing the data flow for that connection for a specified period of time and then comparing the thumbprints for the various connections. If the thumbprints for two host-to-host connections match (within a measure of tolerance), they are mapped to the same extended connection. Thumbprinting even works when the number of intermediate, unmonitored hosts, between two host-to-host connections is unknown *(see* Figure 4).  Figure 4, Tracking a User Across Unmonitored Hosts We formally define a thumbprint for a host-to-host connection as a	[SYM_P_0069250-SYM_P_0069251] "4.2.2 THUMBPRINTS The NSM maps host-to-host connections to an extended connection by assigning to each host-to-host connection a thumbprint representing the data flow for that connection for a specified period of time and then comparing the thumbprints for the various connections. If the thumbprints for two host-to-host connections match (within a measure of tolerance), they are mapped to the same extended connection. Thumbprinting even works when the number of intermediate, unmonitored hosts, between two host-to-host connections is unknown *(see* Figure 4).  Figure 4, Tracking a User Across Unmonitored Hosts We formally define a thumbprint for a host-to-host connection as a

Internetwork Security Monitor
"ISM"

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
		vector, X = <x1, x2, …, xn>, where each xi is a counter for the occurrence of some attribute in the data. Two thumbprints, X and Y, are compared for similarity by determining the distance between the two vectors, I X - Y I. The certainty that the two connections which created the thumbprints are actually part of the same extended connection is inversely related to this magnitude. The mapping of data in a host-to-host connection to a thumbprint vector, although extremely important, is not necessarily uniquely defined, and we are experimenting with various implementations. The implementations are driven by several goals described in Table 1."	vector, X = <x1, x2, …, xn>, where each xi is a counter for the occurrence of some attribute in the data. Two thumbprints, X and Y, are compared for similarity by determining the distance between the two vectors, I X - Y I. The certainty that the two connections which created the thumbprints are actually part of the same extended connection is inversely related to this magnitude. The mapping of data in a host-to-host connection to a thumbprint vector, although extremely important, is not necessarily uniquely defined, and we are experimenting with various implementations. The implementations are driven by several goals described in Table 1."

Internetwork Security Monitor
"ISM"

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
		Table 1. Thumbprint Implementation Goals Resolution: The primary purpose of the thumbprint is to correctly recognize that two host-to-host connections are part of the same extended connection. Semantic Free: As will be seen later, thumbprinting will be used in an open environment where privacy is an issue; therefore, the thumbprint, while being able to represent the connection, should not reveal the contents of the connection data. Efficiency: The calculation of each x_i as well as the calculation of $\|X - Y\|$ must be efficient in order to allow for the thumbprinting of thousands of simultaneous connections and their comparison in real time. (267) [SYM_P_0069249]	Table 1. Thumbprint Implementation Goals Resolution: The primary purpose of the thumbprint is to correctly recognize that two host-to-host connections are part of the same extended connection. Semantic Free: As will be seen later, thumbprinting will be used in an open environment where privacy is an issue; therefore, the thumbprint, while being able to represent the connection, should not reveal the contents of the connection data. Efficiency: The calculation of each x_i as well as the calculation of $\|X - Y\|$ must be efficient in order to allow for the thumbprinting of thousands of simultaneous connections and their comparison in real time. (267) [SYM_P_0069249] "The LAN monitor also uses and maintains profiles of expected network behavior. The profiles consist of expected data paths (e.g., which systems are expected to establish communication paths to

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			which other systems, and by which service) and service profiles (e.g., what a typical *telnet*, *mail*, or *finger* is expected to look like)." (171) [SYM_P_0077179] "Certain critical audit records are always passed directly to the expert system (i.e., *notable events*); others are processed locally by the host monitor (i.e., *profiles* and attack *signatures*, which are sequences of noteworthy events which indicate the symptoms of attacks) and only summary reports are sent to the expert system." (170) [SYM_P_0077178] "The abnormality of a connection is based on the probability of that particular connection occurring and the behavior of the connection itself." (171) [SYM_P_0077179]
	generating, by the monitors, reports of said suspicious activity; and	See '203 claim 1	See '203 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '203 claim 1	See '203 claim 1
2	The method of claim 1, wherein at least one of the network monitors utilizes a signature matching	"Access to this analysis by external ISMs are made by the following requests: • GET ANALYSIS CONN-ID <Id>	"Access to this analysis by external ISMs are made by the following requests: • GET ANALYSIS CONN-ID <Id>

Internetwork Security Monitor
"ISM"

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	detection method.	• GET ANALYSIS HOST-ID <host-address> • GET ANALYSIS SERVICE <service-name> • GET ANALYSIS VULNERABILITY <vulnerability-id> . . . The last request returns a value between 0 and 100 indicating the ISM's belief that a particular vulnerability has recently been exploited. To perform this, the ISM must have a catalog of known vulnerabilities and signatures to detect their [attempted] exploitation. Due to the sensitive nature of vulnerabilities, some ISMs (e.g., those at government sites) may have a more complete listing than other ISMs (e.g., those at universities)." (268-269) [SYM_P_0069250-SYM_P_0069251] "We now present an architecture based on NSM and DIDS which provides for intrusion detection and accountability in large-scale interconnected networks (e.g., the Internet)." (268) [SYM_P_0069250]	• GET ANALYSIS HOST-ID <host-address> • GET ANALYSIS SERVICE <service-name> • GET ANALYSIS VULNERABILITY <vulnerability-id> . . . The last request returns a value between 0 and 100 indicating the ISM's belief that a particular vulnerability has recently been exploited. To perform this, the ISM must have a catalog of known vulnerabilities and signatures to detect their [attempted] exploitation. Due to the sensitive nature of vulnerabilities, some ISMs (e.g., those at government sites) may have a more complete listing than other ISMs (e.g., those at universities)." (268-269) [SYM_P_0069250-SYM_P_0069251] "We now present an architecture based on NSM and DIDS which provides for intrusion detection and accountability in large-scale interconnected networks (e.g., the Internet)." (268) [SYM_P_0069250] "The LAN monitor also uses heuristics in an attempt to identify the likelihood that a particular connection represents intrusive behavior. These heuristics consider the capabilities of each of the network services, the level of authentication required for each of the services, the security level for each machine on the network, and signatures of past attacks." (171) [SYM_P_0077179] "In addition to the consideration of external temporal context, the

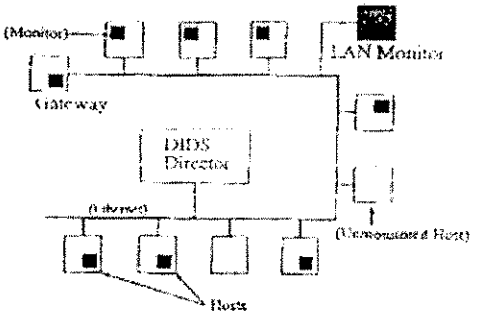
'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			expert system uses time windows to correlate events occurring in temporal proximity. This notion of temporal proximity implements the heuristic that a call to the UNIX *who* command followed closely by a *login* or *logout* is more likely to be related to an intrusion than either of those events occurring alone. Spatial context implies the relative importance of the source of events. That is, events related to a particular user, or events from a particular host, may be more likely to represent an intrusion than similar events from a different source. For instance, a user moving from a low-security machine to a high-security machine may be of greater concern than a user moving in the opposite direction. The model also allows for the correlation of multiple events from the same user or source. In both of these cases, the multiple events are more noteworthy when they have a common element than when they do not." (172) [SYM_P_0077180] "We are designing a signature analysis component for the host monitor to detect events and sequences of events that are known to be indicative of an attack, based on a specific context." (174) [SYM_P_0077182] "The host monitor (Fig. 3) examines each audit record to determine if it should be forwarded to the expert system for further evaluation. Certain critical audit records are always passed directly to the expert system (i.e., *notable events*); others are processed locally by the host monitor (i.e., *profiles* and attack *signatures*,

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			which are sequences of noteworthy events which indicate the symptoms of attacks) and only summary reports are sent to the expert system." (170) [SYM_P_0077178]
3	The method of claim 2, wherein the monitor utilizing a signature matching detection method also utilizes a statistical detection method.	"We now present an architecture based on NSM and DIDS which provides for intrusion detection and accountability in large-scale interconnected networks (e.g., the Internet)." (268) [SYM_P_0069250] "Access to this analysis by external ISMs are made by the following requests: • GET ANALYSIS CONN-ID <Id> • GET ANALYSIS HOST-ID <host-address> • GET ANALYSIS SERVICE <service-name> • GET ANALYSIS VULNERABILITY <vulnerability-id> The first request returns a value between 0 and 100, which indicates whether or not the ISM believes that the user owning the connection given by <id> is behaving intrusively. The second request also returns a value between 0 and 100, indicating whether or not the ISM believes that the host is associated with intrusive activity. The host does not necessarily have to be within the ISM's domain. For example, if one ISM believes it is receiving a number of possibly intrusive connections from a particular host, it can query other ISMs as to whether they believe the host has a hostile	"We now present an architecture based on NSM and DIDS which provides for intrusion detection and accountability in large-scale interconnected networks (e.g., the Internet)." (268) [SYM_P_0069250] "Access to this analysis by external ISMs are made by the following requests: • GET ANALYSIS CONN-ID <Id> • GET ANALYSIS HOST-ID <host-address> • GET ANALYSIS SERVICE <service-name> • GET ANALYSIS VULNERABILITY <vulnerability-id> The first request returns a value between 0 and 100, which indicates whether or not the ISM believes that the user owning the connection given by <id> is behaving intrusively. The second request also returns a value between 0 and 100, indicating whether or not the ISM believes that the host is associated with intrusive activity. The host does not necessarily have to be within the ISM's domain. For example, if one ISM believes it is receiving a number of possibly intrusive connections from a particular host, it can query other ISMs as to whether they believe the host has a hostile

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
		user on it. The third request returns a value between 0 and 100 indicating the ISM's belief that service <service-name> is being used in an unusual and intrusive manner (e.g., when the Internet worm exploited a hole in the mail service). The last request returns a value between 0 and 100 indicating the ISM's belief that a particular vulnerability has recently been exploited. To perform this, the ISM must have a catalog of known vulnerabilities and signatures to detect their [attempted] exploitation. Due to the sensitive nature of vulnerabilities, some ISMs (e.g., those at government sites) may have a more complete listing than other ISMs (e.g., those at universities)." (268-269) [SYM_P_0069250-SYM_P_0069251]	user on it. The third request returns a value between 0 and 100 indicating the ISM's belief that service <service-name> is being used in an unusual and intrusive manner (e.g., when the Internet worm exploited a hole in the mail service). The last request returns a value between 0 and 100 indicating the ISM's belief that a particular vulnerability has recently been exploited. To perform this, the ISM must have a catalog of known vulnerabilities and signatures to detect their [attempted] exploitation. Due to the sensitive nature of vulnerabilities, some ISMs (e.g., those at government sites) may have a more complete listing than other ISMs (e.g., those at universities)." (268-269) [SYM_P_0069250-SYM_P_0069251] "Like the host monitor, the LAN monitor consists of a *LAN event generator* (LEG) and a *LAN agent*. The LEG is currently a subset of UC Davis' NSM [3]. Its main responsibility is to observe all of the traffic on its segment of the LAN to monitor host-to-host connections, services used, and volume of traffic. The LAN monitor reports on such network activity as *rlogin* and *telnet* connections, the use of security-related services, and changes in network traffic patterns." (169) [SYM_P_0077177] "An event reported by a LAN monitor is called a network audit record (nar). The record syntax is: nar(Monitor-ID, Source_Host, Dest_Host, Time, Service, Domain, Status)." (172) [SYM_P_0077180]

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			"The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection." (171) [SYM_P_0077179] "The host monitor (Fig. 3) examines each audit record to determine if it should be forwarded to the expert system for further evaluation. Certain critical audit records are always passed directly to the expert system (i.e., *notable events*); others are processed locally by the host monitor (i.e., *profiles* and attack *signatures*, which are sequences of noteworthy events which indicate the symptoms of attacks) and only summary reports are sent to the expert system." (170) [SYM_P_0077178]
4	The method of claim 1, wherein integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
5	The method of claim 1,	See '203 claim 3	See '203 claim 3

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	wherein integrating further comprises invoking countermeasures to a suspected attack.		
6	The method of claim 1, wherein the plurality of network monitors includes an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
7	The method of claim 1, wherein the enterprise network is a TCP/IP network.	See '203 claim 5	See '203 claim 5
8	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	"An individual site (e.g., a university or government research facility) may contain only a single ISM monitor (e.g., monitoring all traffic in and out of the site), or it may contain many sub-domains, each with its own ISM, divided along department lines." (270) [SYM_P_0069252]	"An individual site (e.g., a university or government research facility) may contain only a single ISM monitor (e.g., monitoring all traffic in and out of the site), or it may contain many sub-domains, each with its own ISM, divided along department lines." (270) [SYM_P_0069252] "In addition to the current host monitor, which is designed to detect attacks on general purpose multi-user computers, we intend to develop monitors for application specific hosts such as file servers and gateways. In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			Network environment." (174) [SYM_P_0077182]  Fig. 1. DIDS Target Environment [SYM_P_0077184]
9	The method of claim 1, wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 8	See '203 claim 8

Internetwork Security Monitor
"ISM"

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
10	The method of claim 9, wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8	See '203 claim 8
11	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
12	The method of claim 11, wherein receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10	See '203 claim 10

Internetwork Security Monitor
"ISM"

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
13	The method of claim 11, wherein the plurality of the domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11
14	An enterprise network monitoring system comprising:	See '212 claim 1	See '212 claim 1
	a plurality of network monitors deployed within an enterprise network;	See '212 claim 1	See '212 claim 1
	said plurality of network monitors detecting suspicious network activity	See '212 claim 1	See '212 claim 1
	based on analysis of network traffic data,	See '212 claim 1	See '212 claim 1
	wherein at least one of the network monitors utilizes a statistical detection method;	See '212 claim 1	See '212 claim 1
	said network monitors generating reports of said suspicious activity; and	See '212 claim 1	See '212 claim 1

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '212 claim 1	See '212 claim 1
15	The system of claim 14, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
16	The system of claim 14, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
17	The system of claim 14, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party	See '203 claim 4	See '203 claim 4

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	tools.		
18	The system of claim 14, wherein the enterprise network is a TCP/IP network.	See '203 claim 5	See '203 claim 5
19	The system of claim 14, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '212 claim 8	See '212 claim 8
20	The system of claim 14, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '212 claim 8	See '203 claim 8
21	The system of claim 20, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's	See '203 claim 8	See '203 claim 8

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.		
22	The system of claim 14, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
23	The system of claim 22, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10	See '203 claim 10
24	The system of claim 22, wherein the plurality of domain monitors within	See '203 claim 11	See '203 claim 11

'212 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	the enterprise network interface as a plurality of peer-to-peer relationships with one another.		

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
1	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	See '203 claim 1	See '203 claim 1
	deploying a plurality of network monitors in the enterprise network;	See '203 claim 1	See '203 claim 1
	detecting, by the network monitors, suspicious network activity	See '203 claim 1	See '203 claim 1
	based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of	See '203 claim 1	See '203 claim 1

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	well-known network-service protocols};		
	generating, by the monitors, reports of said suspicious activity; and	See '203 claim 1	See '203 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '203 claim 1	See '203 claim 1
2	The method of claim 1, wherein integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
3	The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
4	The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
5	The method of claim 1, wherein the enterprise network is a TCP/IP network.	See '203 claim 5	See '203 claim 5
6	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '212 claim 8	See '212 claim 8
7	The method of claim 1, wherein at least one of said network monitors utilizes a statistical detection method.	See '212 claim 1	See '212 claim 1
8	The method of claim 1, wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 8	See '203 claim 8
9	The method of claim 8, wherein receiving and integrating is performed by a domain monitor with respect	See '203 claim 8	See '203 claim 8

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	to a plurality of service monitors within the domain monitor's associated network domain.		
10	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
11	The method of claim 10, wherein receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10	See '203 claim 10
12	The method of claim 10, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships	See '203 claim 11	See '203 claim 11

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	with one another.		
13	An enterprise network monitoring system comprising:	See '615 claim 1	See '615 claim 1
	a plurality of network monitors deployed within an enterprise network,	See '615 claim 1	See '615 claim 1
	said plurality of network monitors detecting suspicious network activity	See '615 claim 1	See '615 claim 1
	based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};	See '615 claim 1	See '615 claim 1

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	said network monitors generating reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '615 claim 1	See '615 claim 1
14	The system of claim 13, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
15	The system of claim 13, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
16	The system of claim 13, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor	See '203 claim 4	See '203 claim 4

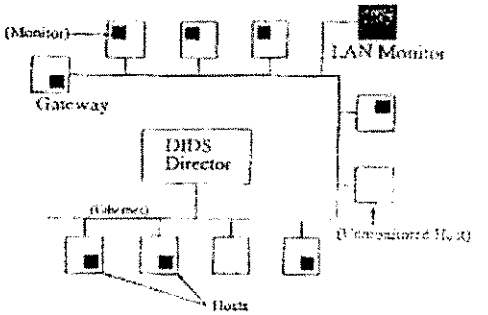
'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	functions and integration of third-party tools.		
17	The system of claim 13, wherein the enterprise network is a TCP/IP network.	See '203 claim 5	See '203 claim 5
18	The system of claim 13, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '212 claim 8	See '212 claim 8
19	The system of claim 13, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 8	See '203 claim 8
20	The system of claim 19, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically	See '203 claim 8	See '203 claim 8

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	receive and integrate the reports of suspicious activity.		
21	The system of claim 13, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
22	The system of claim 21, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10	See '203 claim 10
23	The system of claim 21, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11
34	A computer-automated	See '615 claim 1	See '615 claim 1

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	method of hierarchical even monitoring and analysis within an enterprise network comprising:		
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a gateway;	"An individual site (e.g., a university or government research facility) may contain only a single ISM monitor (e.g., monitoring all traffic in and out of the site), or it may contain many sub-domains, each with its own ISM, divided along department lines." (270) [SYM_P_0069252]	"An individual site (e.g., a university or government research facility) may contain only a single ISM monitor (e.g., monitoring all traffic in and out of the site), or it may contain many sub-domains, each with its own ISM, divided along department lines." (270) [SYM_P_0069252] "In addition to the current host monitor, which is designed to detect attacks on general purpose multi-user computers, we intend to develop monitors for application specific hosts such as file servers and gateways. In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment." (174) [SYM_P_0077182]

Internetwork Security Monitor
"ISM"

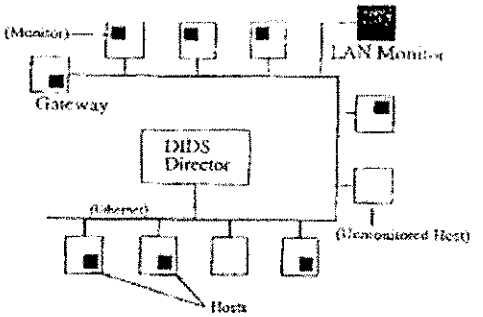
'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			 Fig. 1. DIDS Target Environment [SYM_P_0077184]
	detecting, by the network monitors, suspicious network activity based on analysis of network traffic data;	See '615 claim 1	See '615 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1
	automatically receiving and	See '615 claim 1	See '615 claim 1

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	integrating the reports of suspicious activity, by one or more hierarchical monitors.		
35	The method of claim 34, wherein said integrating comprises correlating intrusion reports reflecting underlying commonalities.	See'203 claim 2	See'203 claim 2
36	The method of claim 34, wherein said integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
37	The method of claim 34, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
38	The method of claim 34, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands,	See '615 claim 1	See '615 claim 1

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.		
39	The method of claim 34, wherein said deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7	See '203 claim 7
40	The method of claim 39, wherein said receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8	See '203 claim 8
41	The method of claim 34, wherein said deploying the network monitors includes deploying a plurality of domain monitors within the	See '203 claim 9	See '203 claim 9

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.		
42	The method of claim 41, wherein said receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10	See '203 claim 10
43	The method of claim 41, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11
44	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:		See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein		"An individual site (e.g., a university or government research facility) may contain only a single ISM monitor (e.g., monitoring all traffic in and out of the site), or it may contain many sub-

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	at least one of the network monitors is deployed at a router;		domains, each with its own ISM, divided along department lines." (270) [SYM_P_0069252] "In addition to the current host monitor, which is designed to detect attacks on general purpose multi-user computers, we intend to develop monitors for application specific hosts such as file servers and gateways. In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment." (174) [SYM_P_0077182]  Fig. 1. DIDS Target Environment [SYM_P_0077184]

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			103: NetRanger: NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-82], 1-6 [SYM_P_0074979], 2-3 to 2-4 [SYM_P_0074996-97]
	detecting, by the network monitors, suspicious network activity based on analysis of the network traffic data;		See '615 claim 1
	generating, by the monitors, reports of said suspicious activity; and		See '615 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.		See '615 claim 1
45	The method of claim 44, wherein said integrating comprises correlating intrusion reports reflecting underlying commonalities.		See '203 claim 2
46	The method of claim 44, wherein said integrating further comprises invoking countermeasures to a		See '203 claim 3

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	suspected attack.		
47	The method of claim 44, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.		See '203 claim 4
48	The method of claim 44, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.		See '615 claim 1
49	The method of claim 44, wherein said deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise		See '203 claim 7

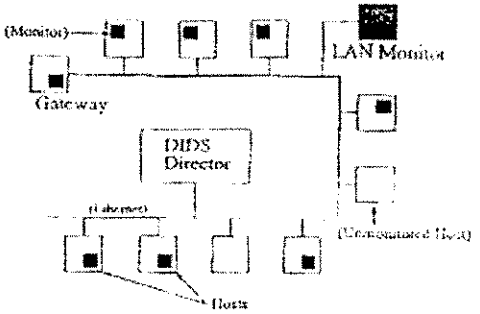
Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	network.		
50	The method of claim 49, wherein said receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.		See '203 claim 8
51	The method of claim 44, wherein said deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.		See '203 claim 9
52	The method of claim 51, wherein said receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.		See '203 claim 10

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
53	The method of claim 51, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.		See '203 claim 11
64	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:		See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a firewall;		**103**: "An individual site (e.g., a university or government research facility) may contain only a single ISM monitor (e.g., monitoring all traffic in and out of the site), or it may contain many sub-domains, each with its own ISM, divided along department lines." (270) [SYM_P_0069252] "In addition to the current host monitor, which is designed to detect attacks on general purpose multi-user computers, we intend to develop monitors for application specific hosts such as file servers and gateways. In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment." (174) [SYM_P_0077182]

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
			 Fig. 1. DIDS Target Environment [SYM_P_0077184] SunScreen Firewall. *See* SunScreen EFS Configuration and Management Guide, Release 1.1 (June 1997) [SUN_0000501-856].
	detecting, by the network monitors, suspicious network activity based on analysis of network traffic data;		See '615 claim 1
	generating, by the monitors,		See '615 claim 1

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	reports of said suspicious activity; and		
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.		See '615 claim 1
65	The method of claim 64, wherein said integrating comprises correlating intrusion reports reflecting underlying commonalities.		See '203 claim 2
66	The method of claim 64, wherein said integrating further comprises invoking countermeasures to a suspected attack.		See '203 claim 3
67	The method of claim 64, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.		See '203 claim 4
68	The method of claim 64, wherein said network traffic data is selected from one or		See '615 claim 1

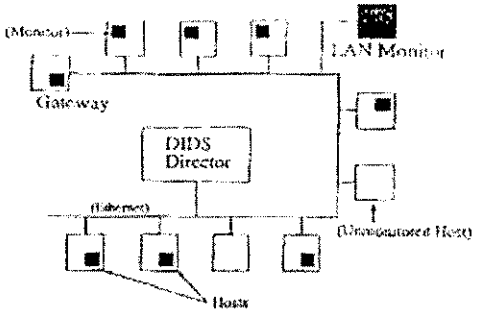
Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.		
69	The method of claim 64, wherein said deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.		See '203 claim 7
70	The method of claim 69, wherein said receiving and integrating is preformed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.		See '203 claim 8
71	The method of claim 64, wherein said deploying the		See '203 claim 9

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.		
72	The method of claim 71, wherein said receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.		See '203 claim 10
73	The method of claim 71, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.		See '203 claim 11
84	An enterprise network monitoring system comprising:	See '615 claim 1	See '615 claim 1
	a plurality of network monitors deployed within an	"An individual site (e.g., a university or government research facility) may contain only a single ISM monitor (e.g., monitoring	"An individual site (e.g., a university or government research facility) may contain only a single ISM monitor (e.g., monitoring

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	enterprise network, wherein at least one of the network monitors is deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers, firewalls}, said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data;	all traffic in and out of the site), or it may contain many sub-domains, each with its own ISM, divided along department lines." (270) [SYM_P_0069252]	all traffic in and out of the site), or it may contain many sub-domains, each with its own ISM, divided along department lines." (270) [SYM_P_0069252] "In addition to the current host monitor, which is designed to detect attacks on general purpose multi-user computers, we intend to develop monitors for application specific hosts such as file servers and gateways. In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment." (174) [SYM_P_0077182]  Fig. 1. DIDS Target Environment [SYM_P_0077184]

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	said network monitors generating reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '615 claim 1	See '615 claim 1
85	The system of claim 84, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
86	The system of claim 84, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
87	The system of claim 84, wherein the plurality of network monitors include an application programming interface (API) for	See '203 claim 4	See '203 claim 4

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	encapsulation of monitor functions and integration of third-party tools.		
88	The system of claim 84, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.	See '615 claim 1	See '615 claim 1
89	The system of claim 84, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7	See '203 claim 7
90	The system of claim 89, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's	See '203 claim 8	See '203 claim 8

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.		
91	The system of claim 84, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
92	The system of claim 91, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10	See '203 claim 10
93	The system of claim 91, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one	See '203 claim 11	See '203 claim 11

Internetwork Security Monitor
"ISM"

'615 Claim number	Claim Term	ISM – 102(b) (printed publication)	ISM / DIDS – 102(b) (incorp. by ref.) / 103 (printed publication)
	another.		